UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: PATRICE HAUSER**,** on behalf of herself and all others similarly situated, Plaintiff, v. GENWORTH LIFE INSURANCE COMPANY, GENWORTH LIFE AND ANNUITY INSURANCE COMPANY, GENWORTH FINANCIAL, INC., PENSION BENEFIT INFORMATION LLC, AND PROGRESS SOFTWARE CORPORATION, Defendants.	MDL No. 1:23-md-03083-ADB-PGL **AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO.: 1:23-cv-12449

Plaintiff Patrice Hauser, individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant Genworth Life Insurance Company ("Genworth"), Genworth Life and Annuity Insurance Company, ("GLAIC"), Genworth Financial, Inc. ("Genworth Financial" and collectively with GLAIC and GLIC, "Genworth"), Pension Benefit Information, LLC ("PBI"), and Progress Software Corporation ("PSC") (collectively, "Defendants"), to obtain damages, restitution, and injunctive relief for the Classes, as defined below, from Defendants. Plaintiff makes the following allegations on information and belief, except as to her own actions, which are made on personal knowledge, the investigation of her counsel, and the facts that are a matter of public record.

INTRODUCTION

1. Plaintiff incorporates the allegations contained in Plaintiffs' Omnibus Statement

of Additional Pleading Facts (ECF No. 908) in its entirety.

2. This class action arises out of the recent targeted cyberattack and data breach, wherein unauthorized third parties accessed Defendants' MOVEit Transfer servers and accessed and removed personal identifiable information ("PII") from the servers as early as May 27, 2023 ("Data Breach").[1] As a result of the Data Breach, Class Members suffered ascertainable losses and are subject to the present and continuing risk of imminent harm caused by the compromise of their sensitive personal information.

3. Defendant Genworth provides financial and insurance services to help customers "navigate caregiving options, protect and grow their retirement income, and prepare for the financial challenges that come as we age."[2]

4. Defendant PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth.

5. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses Defendant PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[3]

6. The specific information that was targeted and compromised in the Data Breach includes Plaintiff's and Class Members' full names, dates of birth, zip codes, states of residence, policy numbers, Social Security numbers, and other sensitive information.

7. Upon information and belief, prior to the Data Breach, Defendants obtained the

[1] The "Website Notice". Available at https://www.genworth.com/moveit.html (last accessed July 19, 2023).
[2] https://www.genworth.com/about-us.html (last accessed July 19, 2023).
[3] https://www.pbinfo.com/ (last visited August 1, 2023).

PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendants' networks, in which unauthorized actors used an extraction tool to retrieve PII from Defendants' networks.

8. Plaintiff's and Class Members' PII—which was entrusted to Defendants, their officials, and agents—was targeted, compromised, and unlawfully accessed due to the Data Breach and Defendants admit that this information was "compromised" from their networks during the Data Breach.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of her and Class Members' PII that Defendants collected and maintained, and for Defendants' failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

10. Defendants maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendants' computer systems and networks in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. Upon information and belief, Defendants and their employees additionally failed to properly monitor the computer networks, IT systems, and integrated services that housed Plaintiff's and Class Members' PII.

12. The cyberattack perpetrated against Defendants was targeted at acquiring the PII stored by Defendants due to its value on internet black markets where it is offered for sale to

identity thieves and fraudsters.

13. As a result of Defendants' negligent conduct, Plaintiff's and Class Members' identities are now at risk because the PII that Defendants collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

14. Defendants failed to provide timely, accurate, and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII that Defendants allowed to be compromised, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendants' failure to warn impacted persons immediately upon learning of the Data Breach.

15. Genworth's Website Notice admitted that the PII accessed included individuals' full names, dates of birth, zip codes, states of residence, policy numbers, Social Security numbers, and other sensitive information.[4]

16. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

17. As a result of the targeted Data Breach, Plaintiff and Class Members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiff and Class Members

[4] *Id.*

must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

18. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

20. Accordingly, Plaintiff brings claims on behalf of herself and the Classes for: (i) negligence; (ii) negligence *per se*; (iii) breach of implied contract; (iv) violation of the Florida Deceptive and Unfair Trade Practices Act; and (v) unjust enrichment. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendants' data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

21. Plaintiff Patrice Hauser is, and at all times mentioned herein was, an individual and citizen of Lakewood Ranch, Florida.

22. Plaintiff Hauser has no intention of moving to a different state in the immediate future. Plaintiff Hauser is acting on her own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Hauser's PII and owe her a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Hauser's PII was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

23. Plaintiff received a notice letter from PBI, on behalf of Genworth, dated July 14,

2023, stating that a data security incident occurred at PBI impacting Genworth, and that Plaintiff's PII was compromised in the incident.

24. Genworth Financial is headquartered in Richmond, Virginia. Genworth Financial, Inc. is a publicly traded Fortune 500 company incorporated in Delaware and headquartered in Richmond, Virginia that trades on the New York Stock Exchange under the trading symbol "GNW." Genworth operates its business through three operating segments: mortgage insurance, long-term care insurance, and life and annuity retirement solutions.

25. Defendant GLIC is a Delaware corporation with its principal place of business located at 6620 West Broad Street, Richmond, Virginia 23230. GLIC is a subsidiary of Genworth Financial.

26. Defendant GLAIC is a subsidiary of Genworth Financial with its principal place of business in Richmond, Virginia.

27. Genworth is a Vendor Contracting Entity of PBI. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

28. Defendant PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, Minnesota 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a "sponsor, administrator, or record keeper" "for thousands of organizations."[5]

29. PBI is a PSC Vendor. (*See* Plfs.' Omnibus Set of Addtl. Pleading Facts, App. A.)

30. Defendant PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Rd, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

[5] www.pbinfo.com (last visited Aug. 1, 2023).

JURISDICTION AND VENUE

31. This case was originally filed in the United States District Court for the Eastern District of Virginia. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

32. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiff, is a citizen of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

33. The United States District Court for the Eastern District of Virginia has general personal jurisdiction over Defendants because Defendant Genworth and/or their parents or affiliates are headquartered in that District. That District has specific personal jurisdiction over all Defendants because they conduct substantial business in Virginia.

34. Venue is proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391(b) because Defendant Genworth's principal places of business are in the District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in that District.

FACTUAL ALLEGATIONS

A. Defendants Collected, Stored, and were Responsible for Protecting Plaintiff's and Class Members' PII.

35. As a condition to taking out long-term care or life insurance policies or annuity contracts with Genworth and receiving other services from Genworth, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendants. According to its Online Privacy Policy, Genworth collects PII from its customers:

- When you contact us:

To ask for general information

To apply for a new policy

To create an account so you can view information about your existing policy

- When we contact you:

To service your policy

To provide information you ask for

To provide information we believe you may be interested in

- When we contact others:

To obtain or confirm information about your (e.g. medical records).[6]

36. Genworth, in turn, provided Plaintiff's and Class Members' PII to PBI in connection with services that PBI rendered to Genworth. The Notice Letter that Plaintiff Hauser received from Genworth reported that "PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions."

37. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Genworth assumed legal and equitable duties and knew or should have known that it was responsible for protecting that PII from unauthorized disclosure.

38. Genworth made repeated assurances to its customers that it was aware of the significant risk and harm associated with failing to safeguard their PII and it had adequate security

[6] Online Privacy Policy, Genworth, https://www.genworth.com/online-privacy-policy.

policies and practices in place to prevent that from happening. Notably, Genworth's Online Privacy Policy stated that "[w]hen you provide information to us on our websites, we use encryption and authentication tools to protect that information after it gets to us."[7] Additionally, "[o]nce we receive your information, we use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards."[8] Genworth further claims to "require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential."[9]

39. In a 2022 Sustainability Report issued by Genworth, the section entitled "Data Protection at Genworth" acknowledged the significant risk of failing to safeguard one's PII, stating that, "[i]n today's increasingly digital world, protecting our own data – and that of our customers and business partners – is essential. Genworth recognizes the significant operational risks, including risk of losses, from cyberattacks and the importance of a strong cybersecurity program for effective risk management."[10]

40. In recognition of these security concerns, Genworth publicly claimed to have a robust data security system in place:

> Our program employs various controls and policies to secure our operations and information including monitoring, reporting, managing, and remediating cybersecurity

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] https://pro.genworth.com/riiproweb/productinfo/pdf/665101C.pdf

threats. Key features of the program include access controls, security training, dedicated security personnel, security event monitoring, and when necessary, consultation with third-party data security experts.

Our IT security program, which is regularly updated to align with best practices and industry guidelines, includes:

• Written IT policies and standards designed to guard the integrity of our institutional, commercial, and private consumers' personal information

• Regular external and internal reviews of our data protection practices

• A robust suite of IT security products that enable us to manage cybersecurity risk within the organization and alternate sites where business is conducted[11]

41. Throughout its website, Genworth reiterates these assurances of security, repeatedly stating that it is aware of data privacy risks and has adequate procedures and process in place to prevent them, such as its statements below:

• "Working to protect your personal information is one of our promises that enables us to help millions of policyholders secure their financial lives, families, and futures."[12]

• "At Genworth, we have implemented technical, physical, and process safeguards to maintain the confidentiality of your information."[13]

• "Genworth uses reasonable administrative, physical and electronic security measures to protect against possible loss, misuse or alteration of Permitted Information or content posted on Bulletin Boards."[14]

[11] *Id.*
[12] https://www.genworth.com/fraud-and-information-protection
[13] *Id.*
[14] https://www.genworth.com/terms-of-use

• "Once we receive your information, we use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards."[15]

• "We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated."[16]

42. PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth.

43. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations", and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[17]

44. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for Genworth.

45. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

[15] *Id.*
[16] *Id.*
[17] https://www.pbinfo.com/ (last visited August 1, 2023).

46. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:

> **9. ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.
>
> **10. IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

47. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiff's and class members' sensitive PII because, inter alia, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

8. ACCOUNTABILITY

PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.

11. COMPLIANCE

PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

48. Discovery will show that through their provision of the foregoing services, PBI obtains possession of customers'—including Plaintiff's and class members'—highly sensitive PII. Thus, in the regular course of their businesses, PBI collects and/or maintains the PII of consumers such as Plaintiff and class members. PBI stores this information digitally in the regular course of business.

49. As evidenced by, inter alia, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiff's and class members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

50. Yet, contrary to PBI's website representations—by virtue of Defendants' admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII entrusted to it. Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII that is entrusted to them.

51. Genworth provides financial and insurance services to help customers "navigate

caregiving options, protect and grow their retirement income, and prepare for the financial challenges that come as we age."[18]

52. Plaintiff and Class Members are current and former Genworth customers who used Genworth for life insurance and/or financial services.

53. In order to obtain insurance and/or financial services at Genworth, Plaintiff and Class Members were required to provide sensitive and confidential PII, including their names, Social Security numbers, dates of birth, addresses, and other sensitive information.

54. The information held by Defendants in its computer systems included the unencrypted PII of Plaintiff and Class Members.

55. Upon information and belief, Defendants made promises and representations to consumers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining products and/or services would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

56. Indeed, Genworth's Privacy Policy provides that: "[o]nce [Defendant] receive[s] your information, [Defendant] use[s] procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. [Defendant] maintain[s] physical, electronic, and procedural protections to protect personal information in accordance with applicable standards."[19]

57. Plaintiff and Class Members provided their PII to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations

[18] https://www.genworth.com/about-us.html (last accessed July 19, 2023).
[19] https://www.genworth.com/online-privacy-policy.html (last accessed July 19, 2023).

to keep such information confidential and secure from unauthorized access.

58. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

59. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to ensure that third parties with whom it shared PII would do the same. Defendants have a legal duty to keep consumers' PII safe and confidential.

60. Defendants had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

61. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

62. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. The Data Breach

63. On or about July 14, 2023, PBI, on behalf of Genworth, began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them, in relevant part, that:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vu1nerabi1ity's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.[20]

64. Omitted from the Notice Letter were the dates of Defendants' investigation into the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

65. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

66. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they collected from Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

67. As a result of Defendants' failure to audit, monitor and verify the integrity of their

[20] The "Notice Letter".

IT vendors, the attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

68. Plaintiff has been informed by Experian that her PII is available on the dark web and further believes that the PII of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

D. Defendants Acquire, Collect, and Store Consumers' PII

69. As a condition to obtain services from Genworth, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendants.

70. Defendants retain and store this information and derive a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendants would be unable to perform their services.

71. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

72. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

73. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

74. Upon information and belief, Defendants made promises to Plaintiff and Class

Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

75. Indeed, Genworth's Privacy Policy provides that: "[o]nce [Defendant] receive[s] your information, [Defendant] use[s] procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. [Defendant] maintain[s] physical, electronic, and procedural protections to protect personal information in accordance with applicable standards."[21]

76. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. The Data Breach was a Foreseeable Risk of which Defendants were on Notice

77. Data thieves regularly target companies like Defendants due to the highly sensitive information that they use in their regular business. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

78. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendants, preceding the date of the breach.

79. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[22]

80. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive

[21] https://www.genworth.com/online-privacy-policy.html (last accessed July 19, 2023).
[22] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

records (9,700,238) in 2020.[23]

81. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

82. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

83. As custodians of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members, and of the foreseeable consequences if their data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

84. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

85. Additionally, as companies became more dependent on computer systems to run

[23] *Id*.

[24] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

their business,[25] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[26]

86. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to potentially thousands or tens of thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

87. In the Notice Letter, PBI makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

88. PBI's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendants' computer systems.

89. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

[25]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html
[26] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

90. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

91. As an insurance company in possession of its customers' and former customers' PII, Genworth knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

F. The Value of Personally Identifiable Information.

92. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[28]

93. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[29] For example, Personal Information can be sold at a price ranging from $40

[27] 17 C.F.R. § 248.201 (2013).
[28] *Id.*
[29] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

to $200.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

94. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[32]

95. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

96. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly

---

[30] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[31] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[32] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

inherited into the new Social Security number."[33]

97. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers and names.

98. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[34]

99. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, home improvement products and/or services, and housing or even give false information to police.

100. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot

[33] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).
[34] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

necessarily rule out all future harm.[35]

101. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

G. Defendants Fail to Comply with FTC Guidelines

102. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

103. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[36] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[37]

104. The FTC further recommends that companies not maintain PII longer than is

[35] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).
[36] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).
[37] *Id*.

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

105. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

106. These FTC enforcement actions include actions against insurance companies, like Genworth.

107. Defendants failed to properly implement basic data security practices.

108. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

109. Defendants were at all times fully aware of their obligation to protect the PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

H. Defendants Fail to Comply with Industry Standards

110. As shown above, experts studying cyber security routinely identify insurance companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

111. Several best practices have been identified that at a minimum should be implemented by insurance companies, like Genworth, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

112. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

113. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

114. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

I. Defendants' Breach

115. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because Defendants failed to ensure that the information shared was properly encrypted while in transit and that their partners used data security practices

appropriate to the nature of information being shared on their computer systems and networks. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII;

c. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

d. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

h. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

i. Failing to train all members of their workforces effectively on the policies and procedures regarding PII;

j. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

k. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5

of the FTC Act;

l. Failing to adhere to industry standards for cybersecurity as discussed above; and,

m. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

116. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves access, which provided unauthorized actors with unsecured and unencrypted PII.

117. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members lost the benefit of the bargain they made with Defendants.

J. Common Injuries and Damages

118. To date, Defendants have done nothing to provide Plaintiff and the Class Members with meaningful relief for the damages they have suffered as a result of the Data Breach.

119. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Plaintiff's & the Class Members' Risk of Identity Theft

120. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

121. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

122. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

123. Plaintiff's and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

124. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.38

[38] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/ (last visited on May 7, 2023).

125. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

126. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

127. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

128. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as PBI’s Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

129. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as replacing credit cards, changing passwords and resecuring their own computer networks, and monitoring their financial accounts for unauthorized

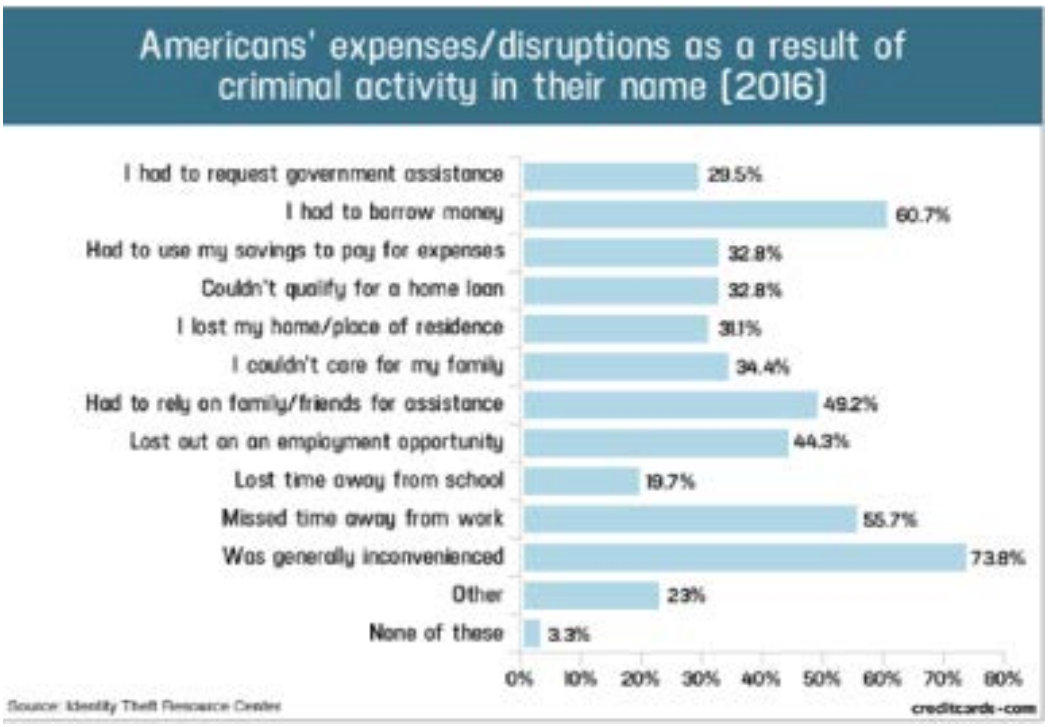
activity, which may take years to discover and detect.

130. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[39]

131. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

132. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[41]

[39] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[40] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[41] Credit Card and ID Theft Statistics" by Patrice Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).



133. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of PII

134. PII is a valuable property right.[42] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

135. Sensitive PII can sell for as much as $363 per record according to the Infosec

[42] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

Institute.[43] An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[44] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[45,46] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[47]

136. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

137. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[43] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[44] *See* Ashiq Ja, *Hackers Selling Financial Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-financial-data-in-the-black-market/ (last visited Sep. 13, 2022).
[45] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[46] https://datacoup.com/
[47] https://digi.me/what-is-digime/

138. The fraudulent activity resulting from the Data Breach may not come to light for years.

139. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

140. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to thousands or tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

141. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit & ID Theft Monitoring is Reasonable & Necessary

142. Given the type of targeted attack in this case, the sophisticated criminal activity, the sensitive type of PII involved in this Data Breach, and Plaintiff's PII already being disseminated on the dark web (as discussed below), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

143. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

144. Consequently, Plaintiff and Class Members are at a continuing risk of fraud and identity theft for many years into the future.

145. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

Loss of Benefit of the Bargain

146. Furthermore, Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendants for insurance and/or financial services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received insurance and/or financial services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

K. Plaintiff Hauser's Experience

147. Plaintiff Hauser received a Notice Letter by U.S. mail addressed to her directly from Genworth, dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses."

148. In order to obtain life insurance from Genworth, Plaintiff Hauser was required to

provide her PII, directly or indirectly, to Genworth, including her name, Social Security number, date of birth, zip code, state of residence, and other sensitive information.

149. At the time that PSC disclosed the Data Breach—on or around May 31, 2023—Defendants retained Plaintiff Hauser's PII in their computer systems.

150. Plaintiff Hauser is very careful about sharing her sensitive PII. She stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. She would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

151. Although Genworth and PBI became aware of the Data Breach on or around May 31, 2023, it took Genworth several months to notify Plaintiff Hauser and other Class Members of the Data Breach's occurrence. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been explained or clarified to Plaintiff Hauser and Class Members, who retain a vested interest in ensuring that their PII remains protected.

152. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

153. As a result of the Data Breach, and at the direction of the Notice Letter, Plaintiff Hauser has spent significant time on making reasonable efforts to mitigate the impact of the Data Breach—valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Specifically, in response to the Data Breach, Plaintiff Hauser has spent significant time on efforts,

including but not limited, to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, enrolling in new credit monitoring services as a result of the Data Breach, monitoring her financial accounts for any indication of additional fraudulent activity, which may take years to detect, and researching notifications she has received about her PII being located on the Dark Web.

154. As a consequence of the Data Breach, Plaintiff Hauser received monthly or bi-monthly notifications from Experian and IDnotify that her PII has been detected on the Dark Web.

155. Plaintiff Hauser further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. As a result of the surge in spam calls Plaintiff Hauser has received since the Data Breach, she had to expend time contracting Spectrum to assist her in trying to block some of the numbers that have repeatedly spammed her and continue to spam her to the present day.

156. Plaintiff Hauser suffered additional injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

157. Moreover, the Data Breach has caused Plaintiff Hauser to suffer fear, anxiety, and

stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

158. As a result of the Data Breach, Plaintiff Hauser is at present risk and will continue to be at increased risk of identity theft and fraudulent activity for years to come.

159. As a result of the Data Breach, Plaintiff Hauser anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm already caused and continue to be caused by the Data Breach.

160. Plaintiff Hauser has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

161. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class Members").

162. Plaintiff sues on behalf of herself and the proposed classes, defined as follows:

(1) PSC Nationwide Class: All persons whose PII was compromised in the MOVEit data breach.

  (a) PSC Florida Class: All residents of Florida whose PII was compromised in the MOVEit data breach.

(2) PBI Nationwide Class: All persons whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

  (a) PBI Florida Class: All residents of Florida whose PII was compromised on PBI's platform and/or systems in the MOVEit data breach.

(3) Genworth Nationwide Class: All persons whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Genworth.

(a) Genworth Florida Class: All residents of Florida whose PII was compromised in the MOVEit data breach where such PII was obtained from or hosted by Genworth.

The foregoing nationwide classes are referred to as the "Nationwide Classes" and the state-specific classes are referred to as the "Florida Classes."

163. Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

164. Plaintiff reserves the right to amend or modify the Class and Subclass definitions and/or add a subclass as this case progresses.

165. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

166. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, on information and belief the each Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

167. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants exercised due diligence in selecting IT vendors and whether Defendants properly audited or monitored the data security systems of third parties with whom they shared PII;

e. Whether Defendants owed a duty to Class Members to safeguard their PII;

f. Whether Defendants breached their duty to Class Members to safeguard their PII;

g. Whether Defendants knew or should have known that their vendors' and partners' data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

168. Typicality. Plaintiff's claims are typical of those of other Class Members because

Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

169. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions.

170. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

171. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

172. Defendants have acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate

on a Class-wide basis.

173. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

174. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

175. Plaintiff re-alleges and incorporates by reference by reference herein all of the

allegations contained in the preceding paragraphs.

176. Defendants require their customers, including Plaintiff and Class Members to submit non-public PII in the ordinary course of providing insurance and/or financial services.

177. Plaintiff and Class Members entrusted Defendants with their PII for the purpose of obtaining insurance and/or financial services from Defendants.

178. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

179. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

180. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Classes entrusted Defendants with their confidential PII, a necessary part of being customers of Defendants.

181. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

182. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Classes.

183. Defendants also had a duty to exercise appropriate clearinghouse practices to

remove former customers' PII they were no longer required to retain pursuant to regulations.

184. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Classes.

185. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations, and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

186. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result

to Plaintiff and the Classes.

187. Defendants' violation of Section 5 of the FTC Act constitutes negligence.

188. Plaintiff and the Classes are within the class of persons that the FTC Act was intended to protect.

189. Defendants' violation of the FTC Act is *prima facie* evidence of negligence.

190. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

191. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Classes was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

192. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

193. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Classes could and would suffer if the PII were wrongfully disclosed.

194. Plaintiff and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Classes, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems.

195. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

196. Plaintiff and the Classes had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

197. Defendants were in a position to protect against the harm suffered by Plaintiff and the Classes as a result of the Data Breach.

198. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Classes within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

199. Defendants admitted that the PII of Plaintiff and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

200. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Classes, the PII of Plaintiff and the Classes would not have been compromised.

201. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes. The PII of Plaintiff and the Classes was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

202. As a direct and proximate result of Defendants' negligence, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web, according to Experian; (ii) invasion of privacy; (iii) lost or

diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

203. As a direct and proximate result of Defendants' negligence, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

204. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

205. Defendants' negligent conduct is ongoing, in that they still hold the PII of Plaintiff and Class Members in an unsafe and insecure manner.

206. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

207. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

208. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs.

209. Plaintiff alleges this negligence *per se* theory as alternative to her other negligence claim.

210. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

211. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

212. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

213. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

214. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

215. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Classes, the PII of Plaintiff and the Classes would not have been compromised.

216. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes. The PII of Plaintiff and the Classes was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

217. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web, according to Experian; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

218. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

219. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long

as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

220. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

221. Defendants' negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

222. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

223. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs.

224. Plaintiff and Class Members were required to provide their PII to Defendants as a condition of obtaining insurance and/or financial services from Defendants.

225. Plaintiff and Class Members provided their PII to Defendants in exchange for (among other things) Defendants' promise to protect their PII from unauthorized disclosure and to delete it once they were no longer required to maintain it.

226. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiff and Class Members that they would only disclose PII under certain circumstances, none of which relate to the Data Breach.

227. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

228. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential, and (g) delete or destroy PII after they were no longer necessary to retain it.

229. When Plaintiff and Class Members provided their PII to Defendants as a condition of receiving insurance and/or financial services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information and to delete or destroy it following the end of the business relationship.

230. Defendants required Class Members to provide their PII as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendants.

231. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security and retention practices complied with relevant representations, laws, and regulations and were consistent with industry standards.

232. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

233. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the implied contract between them and Defendants to delete their PII once it was no longer necessary.

234. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

235. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

236. Defendants breached their implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII.

237. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

238. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

239. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

240. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Violation of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff and the Florida Classes Against All Defendants)

241. Plaintiff re-alleges and incorporates by reference by reference herein all of the

allegations contained in the preceding paragraphs and brings this count on behalf of herself and the Florida Subclasses (the "Classes" for the purposes of this count).

242. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendants obtained Plaintiff's and Class members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff and Class members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

243. As alleged herein this Complaint, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII;

b. failure to make only authorized disclosures of current and former customers' PII;

c. failure to disclose that their data security practices were inadequate to safeguard PII from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members.

244. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Defendants' current and former customers.

245. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Defendants' current and former customers that they did not follow industry best practices for the collection, use, and storage of PII.

246. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to: (i) Plaintiff's PII being disseminated on the dark web, according to Experian; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

247. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

248. Also as a direct result of Defendants' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class members are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendants implement measures that ensure that the PII of Defendants' current and former customers is appropriately encrypted and safeguarded when stored on Defendants' networks or systems;

b. Ordering that Defendants purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;

c. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach

when it occurs and what to do in response to a breach; and

d. Ordering Defendants to meaningfully educate their current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps Defendants' current and former customers must take to protect themselves.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Classes or, Alternatively, the Florida Classes, Against All Defendants)

249. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs.

250. This count is pleaded in the alternative to the breach of implied contract count above (Count III).

251. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for services from Defendants and/or their agents and in so doing also provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their PII protected with adequate data security.

252. Defendants knew that Plaintiff and Class Members conferred a benefit on them in the form of their PII as well as payments made on their behalf as a necessary part of their receiving insurance and/or financial services. Defendants appreciated and accepted that benefit. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

253. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

254. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

255. Defendants, however, failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

256. Defendants would not be able to carry out an essential function of their regular business without the PII of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendants or anyone in Defendants' position would use a portion of that revenue to fund adequate data security practices.

257. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

258. If Plaintiff and Class Members knew that Defendants had not reasonably secured their PII, they would not have allowed their PII to be provided to Defendants.

259. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of

Defendants' decision to prioritize their own profits over the requisite security and the safety of their PII.

260. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

261. Plaintiff and Class Members have no adequate remedy at law.

262. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) Plaintiff's PII being disseminated on the dark web, according to Experian; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; and (vi) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

263. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

264. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and her Counsel to represent the Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands that this matter be tried before a jury.

Dated: June 12, 2024

Respectfully Submitted,

/s/ Kristen A. Johnson

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorneys for Plaintiff and the Proposed Class

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen Johnson
Kristen Johnson